REMARKS

Claims 14-33 are pending in the present application. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

Applicant has amended the claims to overcome the objections and rejection under 35 U.S.C. § 112, second paragraph presented in the final Office Action. Favorable reconsideration is respectfully requested.

Claims 14-33 were rejected under 35 U.S.C. § 103 as being unpatentable over Applicant-admitted prior art in view of Kocher et al (U.S. Patent No. 6,278,783) and Chow et al (U.S Patent No. 6,594,761). This rejection is respectfully traversed for the following reasons.

Claim 14 recites a method of performing a cryptographic protocol between a first electronic entity and a second electronic entity in order to resist an attack against the second electronic entity. The method includes comprising the steps of applying a message to both first and second electronic entities, applying a first chain of operations to the message within the first electronic entity, so as to obtain a result, and determining a second chain of operations from the first chain of operations. The step of determining the second chain of operations from the first chain of operations includes randomly selecting, for at least a part of

the first chain of operations, to perform either the at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or the at least a part of the first chain of operations in a complemented state. The second chain of operations comprises some operations of the first chain of operations which are performed in the same state and some other operations of the first chain of operations which are performed in a complemented state. The method further includes applying the second chain of operations to the message within the second electronic entity so as to obtain a resultant message. The step of applying comprises selecting to output as the resultant message, depending on the step of randomly selecting, one of either the last operation of the second chain of operations in a same state or this last operations of the second chain of operations in a complemented state. The method further includes comparing the resultant message obtained from the second chain of operations to the result of the first chain of operations. This is not taught, disclosed or made obvious by the prior art of record.

The Office Action acknowledges that the admitted prior art does not explicitly disclose "determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly

selecting to perform operations of the first chain in either a normal or a complimented state." Applicant respectfully agrees. The Office Action cites Kocher as allegedly teaching the first deficiency and Chow as allegedly teaching the second deficiency. Applicant respectfully disagrees.

Kocher discloses that,

> unlike traditional DES implementations, which perform a set of processing operations that depend only on the input key in the message, the invention involves additional random (or otherwise unpredictables) state information in the cryptographic processing. The random state information is mixed with the keys, plain text messages, and intermediate quantities used during processing. Col. 2, lines 13-19.

Thus, Kocher is talking about providing additional information in addition to the keys and the message in a random fashion during processing to make it difficult or impossible for attackers to determine the key information.

This portion cited col. 9, lines 1-13 does not contradict this teaching. In the cited section of col. 9, one of ordinary skill in the art would understand that, referring also to col. 6, lines 39-55, a random value K1 (in the case of the key) is produced and K2 is computed as K2=K xOR K1. Next, random permutations K1P and K2P are produced and K1P-inverse is applied K1 and K2P-inverse is applied to K2.

In contrast, according to the present invention, the DES applied to the second entity, comprises two chains of operation. The first chain of operations corresponds to a conventional DES ("applying a first chain of operations to the message within the first electronic entity, so as to obtain a result"). The second chain of operations consists of the same succession of operations, at least some of which have been complemented ("determining a second chain of operations from the first chain of operations"). The second chain of operations is determined, by deciding in a random manner, to execute one or other of the two chains of operations at each generation of any of the messages ("randomly selecting, for at least a part of the first chain of operations, to perform either that at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or the at least a part of the first chain of operations in a complemented state, the second chain of operations comprising some operations of the first chain of operations, which are performed in the same state and some operations of the first chain of operations, which are performed in a complemented state"). Thus, the disclosure of Kocher does not meet the claims of the recitations of Applicant's claimed invention.

Chow does not remedy the deficiencies noted above with respect to Kocher. Chow teaches a way of encoding one n-bit variable into n-boolean variables in which each bit of the original variable is stored in a separate and new boolean variable. Each such boolean variable is either changed or inverted by interchanging true and false. Chow teaches that for bit-wise boolean operations, either the operation the operation or its complement on each bit is performed. There is no disclosure of determining whether or not the complement is to be performed is based on a random determination.

Nor is there a teaching that would suggest modifying Kocher as asserted in the Office Action. It is true that both Kocher and Chow teach ways of increasing leak minimization and tamper resistance of software, including the exchange of cryptographic information. However, the increasing of tamper resistance or leak minimization is an object of the inventions disclosed in the patents, not a teaching that would suggest modification of the teachings in each patent to one of ordinary skill in the art.

For at least these reasons, Applicant respectfully submits that claim 14 is patentable over the prior art of record, whether taken alone or in combination as proposed in the Office Action.

Claims 15-33 depend from and include the recitations of Claim 14. These claims are believed to be patentable in and of themselves and as they depend from and included the recitations of Claim 14, which is patentable for the reasons discussed above.

In view of the above amendments and remarks, Applicant respectfully requests reconsideration and withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to this effect is most earnestly solicited.

If the Examiner has any questions he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant

By 
Ronni S. Jillions
Registration No. 31,979

RSJ:tbs:pap
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\B\Bonn\Akkar1\pto\2005Dec6 PrelAmd.doc